GREGORY A. BROWER
United States Attorney
NANCY J. KOPPE
Assistant United States Attorney
333 Las Vegas Blvd. South, Suite 5000
Las Vegas, NV 89101
702-388-6336

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT MYRON LATHAM, Defendant	2:06-cr-00379-LDG-GWF **GOVERNMENT'S TRIAL MEMORANDUM**

The United States of America, by and through Gregory A. Brower, United States Attorney, and Nancy J. Koppe, Assistant United States Attorney, submits this trial memorandum in the above-referenced matter. Trial is set for September 8, 2008.

Essentially, the case involves the defendant's use of a computer to advertise, transport, receive and possess child pornography.

PROCEDURAL FACTS

On November 15, 2006, a federal Grand Jury sitting in Las Vegas, Nevada, issued an indictment against the defendant Robert Myron Latham, charging him with one count of Transporting Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(1); one count of Receipt of Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(2); and one count of Possession of Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and 2252A(b)(2).

On January 23, 2008, a federal Grand Jury sitting in Las Vegas, Nevada, issued a superseding indictment against the defendant, charging him with Notice to Distribute Child Pornography, in violation of Title 18, United States Code, Section 2251(d)(1)(A), in addition to the prior charges of Transporting, Receipt and Possession of Child Pornography.

On October 9, 2007, the defendant filed a motion to suppress evidence obtained during a search that was executed pursuant to a search warrant. The United States responded to this motion on October 19, 2007, and the defendant replied to the United States' response on October 25, 2007. On November 1, 2007, United States Magistrate Judge George W. Foley, Jr. issued a report and recommendation to deny the defendant's motion to suppress evidence. The defendant filed objections to the Report and Recommendation on November 16, 2007, and the United States filed a motion to strike the defendant's objections on November 19, 2007. On December 3, 2007, the defendant responded to the United States' motion to strike, and on December 10, 2007, the United States replied to the defendant's response. On December 18, 2007, this Court issued an order adopting the Report and Recommendations of Judge Foley and denying defendant's motion to suppress evidence and the United States' motion to strike.

On May 6, 2008, after signing a written plea agreement, defendant appeared before this Court in order to change his plea. Defendant, however, decided he no longer wished to change his plea and withdrew his plea agreement. When the United States stated its intention to use the statements in defendant's plea agreement at trial, his attorney asked to withdraw from the case due to a conflict of interest. This Court appointed current counsel to represent defendant.

On May 7, 2008, defendant filed a motion to reconsider the motion to suppress that was denied by this Court on December 18, 2007. Defendant also filed a motion to suppress the statements he made to the FBI during the execution of the search warrant, based upon a non-binding case that has since been overruled. This Court has denied both motions. On May 7, 2008, the United States filed a motion to admit the facts from the plea agreement. The United States has since agreed that it will admit the facts from the plea agreement only on rebuttal, and only after first consulting with the Court.

On July 22, 2008, defendant filed a motion to dismiss the Indictment. The United States responded to this motion on August 4, 2008. On August 8, 2008, United States Magistrate Judge George W. Foley held an evidentiary hearing on defendant's motion to dismiss. After hearing from defendant's witnesses, Judge Foley stated that he did not need to hear from the witnesses for the United States, as defendant had failed to substantiate his motion with his witnesses. On August 14, 2008, Judge Foley issued a Report and Recommendation, recommending to this Court that defendant's motion to dismiss be denied. On August 18, 2008, defendant objected to the Report and Recommendation, and on August 25, 2008, the United States responded to defendant's objections. This Court has not yet ruled on the motion to dismiss.

The case stands ready for trial as currently scheduled. The Government's case-in-chief should take no more than three days to present.

SUBSTANTIVE FACTS

This case grows out of an investigation aimed at identifying persons sharing child pornography over the Internet via peer to peer (also known as "P2P") file sharing networks. One of the major file sharing programs is "Limewire," which runs on the Gnutella network. Limewire's operations are described at its website, Limewire.com, which describes itself as, "The Official Site for the Fastest File Sharing Program on the Planet." In brief, Limewire allows users to search for, and share, various types of computer files, including movies, videos and pictures. A user may download and install Limewire software on his computer. The user is then able to click on an icon which connects his computer to others using the Gnutella network. Limewire contains a search tool which allows users to input search terms, such as names of files or subject matters. Limewire will then give the user a list of responsive files being shared by computers connected to the network. The list indicates the type, size and names of files, and the speed of the host computer (i.e. the computer containing the file).

A user can select a file, click on it, and thereby connect directly to the host computer. The user can click on a "download" icon, and initiate the transfer of the file to his own computer. The

user may also "browse," or view a directory of all the shared files of the host computer.

A user may also make available files on his computer to others. When a user downloads Limewire, he is given the option of designating the location of the folder which will be available to others. The default folder is the "Shared Files" folder set up by the Limewire software. When a user downloads files, they are placed in the Shared Files folder, which may be browsed and accessed by others using Limewire. A user may transfer the files from his Shared Files folder to any other folder on his hard drive. A user also has the option of turning off the sharing feature, so that none of the files in his computer may be accessed by others.

In February 2005, the Federal Bureau of Investigation (FBI) was involved in an Internet undercover operation (UC) involving peer to peer file sharing. It is known to the FBI that Limewire is frequently used in the trading of child pornography. An agent participating in this operation can connect directly to the publicly-available Gnutella network and conduct text searches for files of interest. Using search terms consistent with images of child sexual abuse typically provides a list that will contain images of child pornography. As the list of files is provided to a participating law enforcement agent, the software used by Gnutella starts seeking additional computers that can share that same file. Once a file has been selected for download, the software displays the IP addresses that have been identified on the Gnutella network as potential contributors to the download. The investigating agent can select an IP address and request a list of other files being offered from this same computer.

Internet computers identify each other by an Internet Protocol (IP) address. IP addresses can assist law enforcement in finding a particular computer on the Internet. By finding out which particular Internet service company issues a particular IP address, the company can then identify the account that used a particular IP address to access the Internet at that precise date and time.

On February 25, 2005, FBI Special Agent (SA) P. Michael Gordon, using an Internet connected computer, launched the P2P Limewire program. SA Gordon conducted a keyword search using the term "r@ygold," which is a term commonly found in the file names of child pornography

images on file sharing networks. SA Gordon viewed the results of the search and observed approximately nineteen matching files available to be viewed and downloaded by others from the computer using the Internet Protocol (IP) address 68.224.236.152. SA Gordon made a screen capture which displayed the names of these files, and a review by FBI SA Andrew Gruninger determined that eight files had names that are indicative of child pornography. SA Gordon then used the Limewire "browse" function to view the names of the approximately 270 image files stored in the share folder of the computer using the IP address 68.224.236.152. A review of the names of these files by SA Gruninger revealed that more than half of them have names that are indicative of child pornography.

Between approximately 2:07 PM Central Standard Time(CST) and 2:24 PM CST, SA Gordon downloaded four (4) image files from the computer using the IP address 68.224.236.152. All four of these files contained images of child pornography. SA Gordon attempted to download a fifth image file from that same computer, but more than half of the image was received from a different computer with a different IP address. That fifth file, which was stored on the target computer, was named, in part, "collection 5...rape 2 THIS IS SICK...illegal preteen underage," and was comprised of thirteen thumbnail-size images of child pornography.

The first image of child pornography downloaded by SA Gordon from the computer using the IP address 68.224.236.152 is named, in part, "PTHC 9yr Girl darkcollection Child Pedo Porn Sex...jpg." This image depicts a naked, juvenile female laying on a bed exposing her anus and genital area. The second image of child pornography downloaded from the computer using the IP address 68.224.236.152 is named, in part, "PTHC Ultra Hard Pedo Child Porn Pedofilia (New) 061...jpg." This image depicts a naked, prepubescent female laying on a bed with an adult male holding a knife near her exposed genital area. Written on the girl's body in what appears to be red cake icing are the words "cut me," "slut," and "hurt me." This image is a known child pornography image. The third image of child pornography downloaded from the computer using the IP address 68.224.236.152 is named, in part, "PTHC Ultra Hard Pedo Child Porn Pedofilia (New) 056...jpg." This image depicts the penis of an adult male pressed against the genital are of a naked, prepubescent female. The fourth

image of child pornography downloaded from the computer using the IP address 68.224.236.152 is named, in part, "Kid-Girl&Mom - BAMBINA-Collection 12-Real Child Porn...jpg." This image depicts a naked adult female pressing a dildo into the genital area of a naked, juvenile female.

During the downloading process, Limewire displayed the source IP address of each image as 68.224.236.152. Additionally, SA Gordon used a software program named CommView to log all the data coming into his computer during the downloading process. CommView is commercially available software for monitoring internet and local network traffic. In addition to multiple other functions, CommView allows the user to view detailed IP connection statistics. SA Gordon reviewed the data logs created by CommView, and determined they also showed that all four of the images of child pornography described in the paragraph above were downloaded from the IP address 68.224.236.152.

A search of the American Registry for Internet Numbers (ARIN) online database indicated that IP address 68.224.236.152 is registered to the Internet service provider (ISP) Cox Communications. An administrative subpoena was served on Cox Communications (Cox) for the subscriber to the IP address 68.224.136.152 during the time period SA Gordon downloaded those four images of child pornography on February 25, 2005. Cox's response to the subpoena listed that IP address as being used by the account of Larry Latham on the date and time that SA Gordon downloaded child pornography images from the IP address.. The response from Cox listed Latham's address as 6420 East Tropicana Avenue, Apartment 164, Las Vegas, Nevada 89122, his telephone number as (702) 898-7339, and it also listed his Social Security number.

Online checks of public information databases, administrative subpoenas to utilities and the DMV, and surveillance further identified Latham as Lawrence E. Latham with date of birth April 9, 1948, with the same Social Security number listed by Cox, and address 6420 East Tropicana Avenue, Trailer 164, Las Vegas, Nevada 89122.

On June 1, 2005, United States Magistrate Judge Lawrence R. Leavitt issued a search warrant for Latham's residence - 6420 East Tropicana Avenue, Unit 164, Las Vegas, Nevada. Judge

Leavitt issued this warrant based on the representations made by SA Gruninger in an accompanying affidavit of probable cause. On June 1, 2005, federal agents executed this search warrant. Investigation at the scene revealed that the residence was occupied by Larry Latham, Larry Latham's brother, defendant Robert Latham, and Larry Latham's estranged wife/defendant's girlfriend, Sherryl Carroll. Pursuant to the search warrant, federal agents seized defendant's laptop computer, as well as the desktop computers belonging to Larry Latham and Sherryl Carroll. A forensic examination of Larry Latham and Sherryl Carroll's computers revealed no contraband. A forensic examination of defendant's computer, however, revealed a large number of child pornography images. Many of these images were saved in well-organized folders labeled by name or category. Additionally, defendant's computer contained known child pornography images, as well as child pornography images depicting prepubescent children, and sadistic and masochistic images. This child pornography was not produced in Nevada.

LAW AND PROOF

The precise elements of the offenses are set forth in the government's proposed jury instructions. Essentially, the government will prove the defendant's guilt by establishing that the defendant utilized a computer and computer media to connect to Limewire, advertise child pornography, transport child pornography, and receive and possess child pornography.

With respect to the advertising charge, the government will prove that the defendant knowingly made or published, or caused to be made or published, any notice offering to exchange, display, distribute and reproduce any visual depiction, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct, and such notice was transported in interstate or foreign commerce by any means including by computer.

With respect to the transporting child pornography charge, the government will prove that the defendant knowingly transported or shipped in interstate or foreign commerce by any means including by computer, any child pornography.

With respect to the receipt of child pornography charge, the government will prove that the defendant knowingly received any child pornography that has been mailed, shipped or transported in interstate or foreign commerce by any means, including by computer, or any material that contains child pornography that has been mailed, shipped or transported in interstate or foreign commerce by any means, including by computer.

With respect to the possession of child pornography charge, the government will prove that the defendant knowingly possessed any book, magazine, periodical, film, videotape, computer disk, or any other material containing an image of child pornography, that had been mailed, shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped or transported in interstate or foreign commerce by any means, including by computer.

WITNESS LIST AND EXHIBIT LIST

The witness list and the exhibit list will be filed separately. The government anticipates calling approximately eight witnesses and introducing several exhibits.

EVIDENTIARY ISSUES

The defendant signed a plea agreement, which has a provision stating that

> In exchange for the United States entering into this agreement, defendant agrees that (a) the facts set forth in Section IV of this Plea Agreement shall be admissible against defendant under Fed. R. Evidence. 801(d)(2)(A) in the following circumstances: (1) for any purpose at sentencing; and (2) in any subsequent proceeding, including a trial in the event defendant does not plead guilty or withdraws defendant's guilty plea, to impeach or rebut any evidence, argument or representation offered by or on defendant's behalf; and (b) defendant expressly waives any and all rights under Fed. R. Criminal P. 11(f) and Fed. R. Evid. 410 with regard to the facts set forth in Section IV of the Plea Agreement to the extent set forth above.

Since defendant did not plead guilty, the United States has filed a motion with the Court asking to use the facts in Section IV against defendant at trial. The United States has since represented to this Court that it will only use these facts on its rebuttal case, and only after consulting with the Court. The United States submits that, as stated in the plea agreement, it can use these facts to "impeach or rebut

any evidence, argument or representation offered by or on defendant's behalf," and it will ask the Court to allow it to do so if defendant presents any evidence, argument or representation that runs contrary to these facts.

CERTIFICATE OF READINESS FOR TRIAL

The undersigned hereby certifies that she is the trial counsel for the United States herein; that subpoenas have been issued for all non-governmental employees who will testify herein, and that the matter is ready for trial on the date set.

DATED this 26th day of August, 2008.

Respectfully submitted,

GREGORY A. BROWER
United States Attorney

/s/
NANCY J. KORPE
Assistant United States Attorney

This is to certify that the foregoing Government's Trial Memorandum will be personally served upon defense counsel prior to commencement of trial.

DATED this 26th day of August, 2008.

Respectfully submitted,

GREGORY A. BROWER
United States Attorney

/s/
NANCY J. KOPPE
Assistant United States Attorney